

# LIFTS, DERANDOMIZATION, AND DIAMETERS OF SCHREIER GRAPHS OF MEALY AUTOMATA

ANTON MALYSHEV\* AND IGOR PAK\*

**ABSTRACT.** It is known that random 2-*lifts* of graphs give rise to expander graphs. We present a new conjectured derandomization of this construction based on certain *Mealy automata*. We verify that these graphs have polylogarithmic diameter, and present a class of automata for which the same is true. However, we also show that some automata in this class do not give rise to expander graphs.

## 1. INTRODUCTION

In [BL], Bilu and Linial showed that random 2-*lifts* of expanding graphs remain expanding with high probability. This gives a probabilistic construction of expander families. Several ways to derandomize this procedure are also given in [BL], but none of them give a *strongly explicit* description of a family of expander graphs. That is, a description in which the actual graph is much larger than working memory, but a computer can list neighbors of a vertex in polylogarithmic (in the size of the graph) time.

We consider the following two families of 2-*lifts* of graphs. The *Aleshin graphs*  $A_0, A_1, A_2, \dots$  are a sequence of 3-regular edge-labeled directed graphs. The first graph  $A_0$  is defined to be a single vertex with three self-loops labeled  $a, b$ , and  $c$ . Given the graph  $A_n$ , the next graph  $A_{n+1}$  is defined as a certain *graph lift* of  $A_n$ : Each vertex  $v \in A_n$  lifts to two vertices  $v_0, v_1 \in A_{n+1}$ , and the edges transform as follows:

$$\begin{array}{lll} v \xrightarrow{a} w & \text{lifts to} & \begin{array}{l} v_0 \xrightarrow{c} w_0 \\ v_1 \xrightarrow{c} w_1 \end{array} \\ v \xrightarrow{b} w & \text{lifts to} & \begin{array}{l} v_0 \xrightarrow{a} w_0 \\ v_1 \xrightarrow{b} w_1 \end{array} \\ v \xrightarrow{c} w & \text{lifts to} & \begin{array}{l} v_0 \xrightarrow{b} w_0 \\ v_1 \xrightarrow{a} w_1 \end{array} \end{array}$$

That is, e.g., if  $A_n$  has an edge labeled  $c$  from  $v$  to  $w$ , then  $A_{n+1}$  has an edge labeled  $b$  from  $v_0$  to  $w_1$ , and an edge labeled  $a$  from  $v_1$  to  $w_0$ .

Another family, the *Bellaterra graphs*  $B_0, B_1, B_2, \dots$  is defined the same way, except with transformation rules

$$\begin{array}{lll} v \xrightarrow{a} w & \text{lifts to} & \begin{array}{l} v_0 \xrightarrow{c} w_0 \\ v_1 \xrightarrow{c} w_1 \end{array} \\ v \xrightarrow{b} w & \text{lifts to} & \begin{array}{l} v_0 \xrightarrow{a} w_0 \\ v_1 \xrightarrow{b} w_1 \end{array} \\ v \xrightarrow{c} w & \text{lifts to} & \begin{array}{l} v_0 \xrightarrow{b} w_0 \\ v_1 \xrightarrow{a} w_1 \end{array} \end{array}$$

---

\*Department of Mathematics, UCLA, Los Angeles, CA, 90095. Email: {amalyshev,pak}@math.ucla.edu.

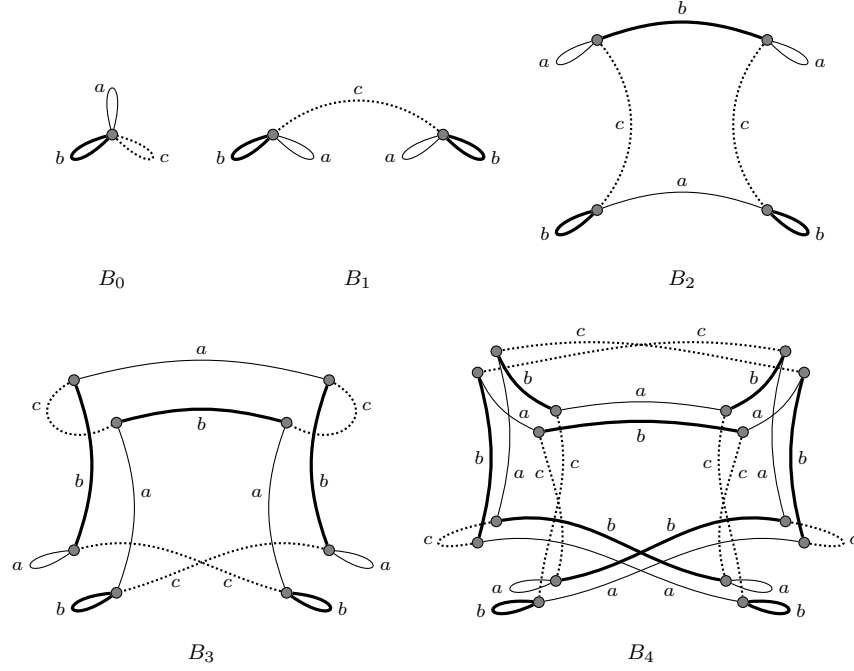


FIGURE 1. The Bellaterra graphs

It is not hard to check that the reverse of every edge in  $B_n$  is also in  $B_n$ , so these can be thought of as undirected graphs. The first few graphs in this family are pictured in Figure 1.

The main result of this paper is the following theorem:

**Theorem 1.1.** *The diameter of the Aleshin graphs  $\{A_i\}_{i=1}^{\infty}$  and Bellaterra graphs  $\{B_i\}_{i=1}^{\infty}$  grows at most quadratically in  $n$ , i.e.,*

$$\text{diam}(A_n) = O(n^2) \quad \text{and} \quad \text{diam}(B_n) = O(n^2) \quad \text{as } n \rightarrow \infty.$$

Prior to this paper, there were no nontrivial bounds on the diameter of  $A_n$ ; even subexponential bounds remained out of reach. Note also that in principle we can start with *any* 3-labeled graph in place of  $A_0 = B_0$ , and proceed making lifts as above. We do not consider these in the paper, and our algebraic techniques do not apply.

Observe that both families of graphs are *very explicit* in the following sense: there is a polynomial time algorithm which, given a number  $n$  and  $v \in \Gamma_n$ , lists the neighbors of  $v$ . “Polynomial time” here refers to a runtime which is polynomial in the number of bits necessary to describe the input. It takes  $n$  bits to describe a vertex of  $B_n$  or  $A_n$ , so the algorithm should run in time  $O(n^d)$ , for some  $d$ .

In particular, it follows that they are *strongly explicit* in the sense of [BL]: There is a polynomial time (in the size of the inputs) algorithm which, given a number  $n$ , and vertices  $v, w \in \Gamma_n$ , decides whether  $v$  and  $w$  are adjacent in  $\Gamma_n$ .

As we will see below, these graphs can be described in terms of invertible *Mealy automata*. The associated automata are small: they act on binary strings and have only 3 states. A detailed study of all such small automata was performed in [B+]. The Bellaterra and Aleshin automata are numbered 846 and 2240 in that article. They are the only nontrivial *bireversible* ones. Spectra of the first few associated graphs are also computed in [B+], and the data suggest that the Aleshin graphs are a family of expanders with eigenvalue gap roughly 0.2.

**Conjecture 1.2.** *The Aleshin graphs  $\{A_i\}_{i=1}^{\infty}$  are a family of two-sided expanders.*

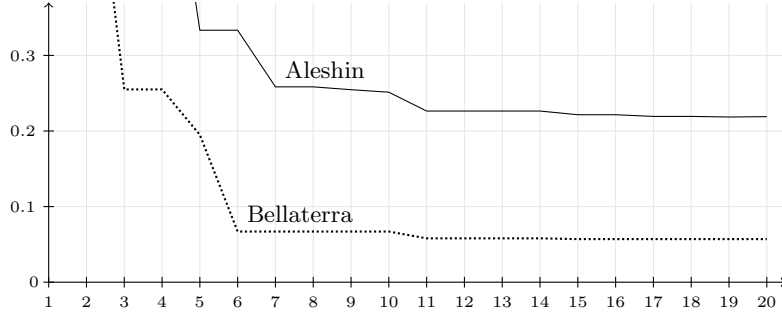


FIGURE 2. Eigenvalue gaps of the Bellaterra and Aleshin graphs.

Here by *two-sided* we mean that both the second largest and the smallest eigenvalues of 3-regular graphs  $A_n$  are bounded away as follows:  $\lambda_2 < 3 - \varepsilon$  and  $\lambda_n > -3 + \varepsilon$  (see e.g. [Tao]).

Though it is less clear from the data in [B+], our own computations (see Figure 2) suggest that the Bellaterra graphs are also expanders, with eigenvalue gap roughly 0.05, so we make the stronger conjecture:<sup>1</sup>

**Conjecture 1.3.** *The Bellaterra graphs  $\{B_i\}_{i=1}^\infty$  are a family of two-sided expanders.*

If so, they are a strongly explicit derandomization of the probabilistic construction in [BL]. One consequence of being an expander family is logarithmic diameter growth with respect to the size of the graph, so if Conjecture 1.2 holds then  $\text{diam}(A_n)$  grows linearly in  $n$ , stronger claim than in the theorem.

Unfortunately, we are not near proving either conjectures and in fact our tools are too weak to prove them. Later in the paper, we state and prove general conditions on an automaton which guarantee polynomial diameter growth in the associated graphs (Section 8). We then prove that for some automata which satisfy those conditions, we do not get expanders (see Section 10). In other words, a different, perhaps combinatorial technique is needed to prove the expansion.

## 2. MEALY AUTOMATA

The Bellaterra graphs  $\{B_n\}_{n=1}^\infty$  are *very explicit* in the sense of [HLW].<sup>2</sup> That is, there is a polynomial time algorithm which, given a number  $n$  and a vertex  $v \in B_n$ , lists the neighbors of  $v$  in  $B_n$ . It takes  $n$  bits to describe a vertex in  $B_n$ , so the runtime of the algorithm should be polynomial in  $n$ .

In fact, there is a linear time algorithm. Even more strongly, the computation can be implemented with a Mealy automaton, i.e., a finite state automaton which outputs a letter each time it reads a letter.

**Definition 2.1.** A *Mealy automaton*  $\mathcal{M} = (Q, A, \tau, \sigma)$  is a pair of finite sets  $Q, A$ , together with functions  $\sigma : Q \times A \rightarrow A$ , and  $\tau : Q \times A \rightarrow Q$ .

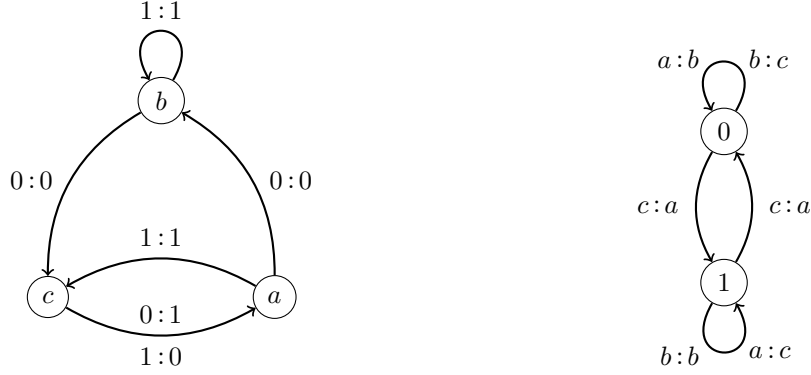
The sets  $Q$  and  $A$  are called the *states* and *alphabet*, respectively. The functions  $\sigma$  and  $\tau$  are called the *output* and *transition* functions, respectively. When  $|Q| = q$  and  $|A| = a$ , we call  $\mathcal{M}$  a  $(q, a)$ -automaton. We adopt the following notations:

$$\begin{aligned} {}^q x &= \sigma_q(x) = \sigma(q, x) \\ q^x &= \tau_x(q) = \tau(q, x). \end{aligned}$$

Let  $A^*$  and  $A^\infty$  denote the set of finite and infinite words in the alphabet  $A$ , respectively, and let  $A^{*,\infty} = A^* \cup A^\infty$  denote the set of all words in  $A$ . A Mealy automaton in the state  $q \in Q$  acts in a

<sup>1</sup>See Remark 11.2.

<sup>2</sup>Sometimes, these are called *fully explicit*, see e.g. [Vad].

FIGURE 3. The Bellaterra automaton  $\mathcal{B}$  and its dual  $\bar{\mathcal{B}}$ 

length-preserving way on words in  $A^{*,\infty}$  by reading the first letter  $x$ , outputting the letter  $\sigma(q, x)$ , and acting on the rest of the word from the state  $\tau(q, x)$ . That is, each  $q \in Q$  has a corresponding length-preserving map  $A^{*,\infty} \rightarrow A^{*,\infty}$  defined recursively by

$${}^q(x_0x_1 \dots x_n) = y_0 {}^r(x_1 \dots x_n),$$

$$\text{and } {}^q(x_0x_1x_2 \dots) = y_0 {}^r(x_1x_2 \dots),$$

where  $y_0 = \sigma(q, x_0)$  and  $r = \tau(q, x_0)$ . This extends to a left action of finite words  $Q^*$  on words in  $A^{*,\infty}$  via, e.g.,

$${}^{qr}s = {}^q({}^rs).$$

So we've defined an extension of  $\sigma : Q \times A \rightarrow A$  to a map  $\sigma : Q^* \times A^{*,\infty} \rightarrow A^{*,\infty}$  given by

$$\sigma(w, s) = \sigma_w(s) = {}^ws.$$

A Mealy automaton can be depicted with a Moore diagram: a directed graph with a vertex for each state  $q \in Q$  and a labeled edge

$$q \xrightarrow{x:y} r$$

for every  $q \in Q$  and every  $x \in A$ , where  $y = \sigma(q, x)$  and  $r = \tau(q, x)$ . That is, an edge  $q \xrightarrow{x:y} r$  denotes that if the Mealy automaton is in state  $q$  and reads the letter  $x$ , then it outputs the letter  $y$  and transitions to the state  $r$ . We will sometimes simply write  $q \xrightarrow{x:y} r$  to denote that  $y = \sigma(q, x)$  and  $r = \tau(q, x)$ .

**Example 2.2.** Consider the *Bellaterra automaton*  $\mathcal{B}$  pictured in Figure 3. More formally,  $\mathcal{B} = (Q, A, \tau, \sigma)$  is defined by

$$A = \{0, 1\}, \quad Q = \{a, b, c\}$$

$$\sigma_a = \sigma_b = (0)(1), \quad \sigma_c = (0 \ 1),$$

$$\text{and } \tau_0 = (a \ b \ c), \quad \tau_1 = (a \ c)(b),$$

where we use the usual cycle notation for permutations, so e.g.,  $\tau_0(a) = b$ ,  $\tau_0(b) = c$ ,  $\tau_0(c) = a$ .

Then given a number  $n$ , the Bellaterra graph  $B_n$  can be described as the graph whose vertices are length  $n$  binary strings, with an edge

$$s \xrightarrow{q} ({}^qs)$$

for each vertex  $s \in A^n$  and each state  $q \in Q$ . For example, we have

$${}^c(0000) = 1 \ {}^a(000) = 10 \ {}^b(00) = 100 \ {}^c(0) = 1001,$$

$$\text{so } 0000 \xrightarrow{c} 1001.$$

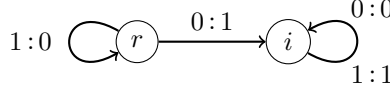


FIGURE 4. The binary adding machine

Some symmetry between states and letters of a Mealy automaton is already apparent in the definition. The nature of this symmetry becomes more clear if we consider computing compositions of maps associated to the states of an automaton, we have, e.g.,

$$q_1 q_0(x_0 x_1 \dots x_n) = q_1(y_0 \overset{r_0}{\rightarrow}(x_1 \dots x_n)) = z_0 \overset{r_1 r_0}{\rightarrow}(x_1 \dots x_n) = \dots,$$

where  $q_0 \xrightarrow{x_0:y_0} r_0$ , and  $q_1 \xrightarrow{y_0:z_0} r_1$ . The computation proceeds by taking any instance of  $q(x \dots)$  in the expression, and replacing it with  $y \overset{r}{\rightarrow}(\dots)$ , where  $q \xrightarrow{x:y} r$ .

If we ignore parentheses, states in  $Q$  and letters in  $A$  play a symmetric role in this process, except that letters in  $Q$  are written higher and disappear when they are at the right side of the expression. Taking this symmetry into account, the automaton also naturally defines an action of the letters in  $A$  on finite words in  $Q^*$ :

$$(q_n \dots q_1 q_0)^x = (q_n \dots q_1)^y r_0,$$

where  $q_0 \xrightarrow{x:y} r_0$ . Letters in  $A$  also act on the set of *left*-infinite words in the alphabet  $Q$ :

$$(\dots q_2 q_1 q_0)^x = (\dots q_2 q_1)^y r_0.$$

We let  $Q^{-\infty}$  denote this set of left-infinite words, and let  $Q^{-\infty,*}$  denote  $Q^* \cup Q^{-\infty}$ , so we have an action of  $A$  on  $Q^{-\infty,*}$ . This naturally extends to a *right* action of  $A^*$  on  $Q^{-\infty,*}$ , via, e.g.

$$w^{xy} = (w^x)^y.$$

So we have defined a map  $\tau : Q^{-\infty,*} \times A^* \rightarrow Q^{-\infty,*}$ , given by

$$\tau(w, s) = \tau_s(w) = w^s.$$

It is straightforward to check that for any  $s \in A^*, t \in A^{*,\infty}, w \in Q^*, v \in Q^{-\infty,*}$ , the actions we have defined satisfy the following relations:

$$\begin{aligned} w(st) &= \tilde{s} \tilde{w}(t), \quad \text{and} \\ (vw)^s &= (v)^{\tilde{s}} \tilde{w}, \end{aligned}$$

where  $\tilde{s} = w^s$  and  $\tilde{w} = w^s$ .

If we need to specify the automaton, we will write  $\sigma_{\mathcal{M}} = \sigma$  and  $\sigma_{\mathcal{M},w} = \sigma_w$ , and similarly for  $\tau$ .

With this symmetry in mind, it is sensible to define the *dual* of an automaton  $\mathcal{M} = (Q, A, \tau, \sigma)$  to be the automaton  $\overline{\mathcal{M}} = (\widehat{Q}, \widehat{A}, \widehat{\tau}, \widehat{\sigma})$  given by interchanging the roles of the states and alphabet. That is, we take

$$\widehat{A} = Q, \quad \widehat{Q} = A, \quad \widehat{\sigma}(a, q) = \tau(q, a), \quad \text{and} \quad \widehat{\tau}(a, q) = \sigma(q, a).$$

In other words, for  $q, r \in Q$  and  $x, y \in A$ , we have  $x \xrightarrow{q:r} y$  in  $\overline{\mathcal{M}}$  if and only if  $q \xrightarrow{x:y} r$  in  $\mathcal{M}$ .

Computations in the dual automaton are computations in the original automaton, with each step written backwards. It follows that, e.g., for every  $s \in A^*$  and  $w \in Q^*$  we have

$$\sigma_{\overline{\mathcal{M}}}(s, w) = \overline{\tau_{\mathcal{M}}(\overline{w}, \overline{s})},$$

where  $\overline{u}$  denotes the reversal of  $u$ .

**Example 2.3.** The dual of the Bellaterra automaton is also pictured in Figure 3.

**Example 2.4.** Let  $A = \{0, 1\}$ . Consider the Mealy automaton pictured in Figure 4. The map  $\sigma_r : \{0, 1\}^* \rightarrow \{0, 1\}^*$  is simply addition of 1, where length  $n$  words in  $A^*$  are interpreted as binary representations of numbers modulo  $2^n$ , with the least significant digit on the left.

We say a Mealy automaton is *invertible* if  $\sigma_q$  is invertible for every  $q \in Q$ . This occurs if and only if the endomorphism  $\sigma_w : A^* \rightarrow A^*$  is invertible for every  $w \in Q^*$ . We are primarily interested in invertible automata, though our results can be generalized to the non-invertible case.

The *inverse* of an invertible automaton  $\mathcal{M} = (Q, A, \tau, \sigma)$  is the automaton  $\mathcal{M}^{-1} = (Q', A, \tau', \sigma')$  given by

$$Q = \{q' \mid q \in Q\}, \quad \sigma'_{q'} = \sigma_q^{-1}, \quad \tau'(q', a) = \tau(q, \sigma_q^{-1}(a)).$$

It is straightforward to check that  $\sigma_{\mathcal{M}^{-1}, q'} = \sigma_{\mathcal{M}, q}^{-1}$  for every  $q \in Q$ .

Consider two automata  $\mathcal{M} = (Q, A, \tau, \sigma)$ ,  $\mathcal{M}' = (Q', A, \tau', \sigma')$  acting on the same alphabet, with  $Q, Q'$  disjoint. Their *union* is the automaton  $\mathcal{M} \cup \mathcal{M}' = (Q \cup Q', A, \tau'', \sigma'')$ , where

$$\tau''(q, a) = \begin{cases} \tau(q, a) & q \in Q \\ \tau'(q, a) & q \in Q' \end{cases} \quad \text{and} \quad \sigma''(q, a) = \begin{cases} \sigma(q, a) & q \in Q \\ \sigma'(q, a) & q \in Q' \end{cases}$$

For example,  $\mathcal{M} \cup \mathcal{M}^{-1}$  is an automaton with twice as many states as  $Q$ , in which every state  $q$  has an inverse state  $q'$  with  $\sigma_{q'} = \sigma_q^{-1}$ .

We say an automaton is *reversible* if its dual is invertible.

We say an automaton is *bireversible* if it is invertible, reversible, and its inverse is reversible. Note that the last condition does not follow from the other two. For example, the three-state automaton in Figure 8 is reversible and invertible, but not bireversible.

### 3. SCHREIER GRAPHS

For our purposes, graphs are locally finite, directed, and may have self-loops and repeated edges. A graph is *regular* if the indegree and outdegree are the same across all vertices.

Let  $\Gamma$  be a graph. Given vertices  $v, w \in \Gamma$ , we write  $v \rightarrow_{\Gamma} w$  if there is an edge in  $\Gamma$  from  $v$  to  $w$ . We write  $d_{\Gamma}(v, w)$  for the distance between  $v$  and  $w$ , i.e. the length of the shortest undirected path between  $v$  and  $w$ . When there is no such path, we take  $d_{\Gamma}(v, w) = \infty$ . Given a nonnegative integer  $r$ , the *ball* of radius  $r$  centered at  $v$  is the set

$$B_{\Gamma}(v, r) = \{w \in \Gamma : d(v, w) \leq r\}.$$

The *diameter* of  $\Gamma$  is defined to be

$$\text{diam}(\Gamma) = \max_{v, w \in \Gamma} d_{\Gamma}(v, w).$$

When it is clear from context what graph we are discussing, we will drop the subscripts and simply write  $v \rightarrow w$ ,  $d(v, w)$ , and  $B(v, r)$ .

In Example 2.2 we described the Bellaterra graphs in terms of a Mealy automaton. In the same way, we can associate a sequence of graphs to any Mealy automaton. Since we are primarily concerned with regular graphs, we require the automaton to be invertible.

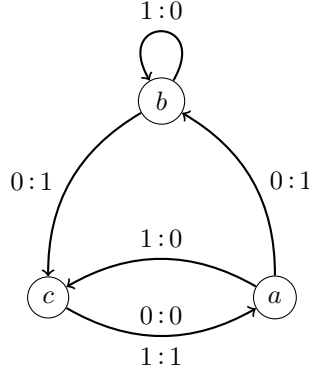
**Definition 3.1.** Let  $\mathcal{M} = (Q, A, \sigma, \tau)$  be an invertible Mealy automaton. Given  $n \in \{1, 2, \dots\} \cup \{\infty\}$ , the *Schreier graph*  $\Gamma_{\mathcal{M}, n}$  is a directed graph, defined as follows: The vertices of  $\Gamma_{\mathcal{M}, n}$  are length  $n$  words in  $A^{*, \infty}$ , i.e. elements of  $A^n$ . For each vertex  $s \in \Gamma_{\mathcal{M}, n}$  and each state  $q \in Q$ , the Schreier graph  $\Gamma_{\mathcal{M}, n}$  has an edge

$$s \rightarrow q_s.$$

Clearly, the number of edges leaving a vertex is  $|Q|$ . The Schreier graph of the inverse automaton,  $\Gamma_{\mathcal{M}^{-1}, n}$ , is simply  $\Gamma_{\mathcal{M}, n}$  with the edges reversed. So, the number of edges entering a given vertex in  $\Gamma_{\mathcal{M}^{-1}, n}$  is also  $|Q|$ , and  $\Gamma_{\mathcal{M}, n}$  is regular.

**Example 3.2.** The  $n$ -th Bellaterra graph  $B_n$  is the Schreier graph  $\Gamma_{\mathcal{B}, n}$ , where  $\mathcal{B}$  is the Bellaterra automaton, pictured in Figure 3.

**Example 3.3.** The  $n$ -th Aleshin graph  $A_n$  is the Schreier graph  $\Gamma_{\mathcal{A}, n}$ , where  $\mathcal{A}$  is the Aleshin automaton, first considered in [A], pictured in Figure 5.

FIGURE 5. The Aleshin automaton  $\mathcal{A}$ 

#### 4. AUTOMATON GROUPS

Let  $\mathcal{M} = (Q, A, \tau, \sigma)$  be an invertible Mealy automaton. As seen in Section 2, we have invertible maps  $\sigma_q : A^{*,\infty} \rightarrow A^{*,\infty}$  for each  $q \in Q$ . This gives an action of the free group  $F_Q$  on  $A^{*,\infty}$ . We can extend the definition of  $\sigma$  as follows: For  $w \in F_Q$ , we can define  $\sigma_w$  in the natural way, e.g.,

$$\sigma_{qr^{-1}} = \sigma_q \sigma_r^{-1}.$$

As usual, we will adopt the notational convention

$$\sigma_w(s) = \sigma(w, s) = {}^w s.$$

The *automaton group* associated to  $\mathcal{M}$  is the group  $G_{\mathcal{M}}$  generated by the automorphisms  $\sigma_q$ .

For example, letting  $\mathcal{A}$  denote the Aleshin automaton, it was shown in [VV] that  $\sigma_{\mathcal{A},a}$ ,  $\sigma_{\mathcal{A},b}$ , and  $\sigma_{\mathcal{A},c}$  satisfy no nontrivial relation, so  $G_{\mathcal{A}}$  is the free group  $F_3$ . However, it is straightforward to check that  $\sigma_{\mathcal{B},a}^2 = \sigma_{\mathcal{B},b}^2 = \sigma_{\mathcal{B},c}^2 = \text{id}$ , where  $\mathcal{B}$  is the Bellaterra automaton. It can be shown (see, e.g., [Nek, B+]) that the words satisfy no other relation, so we say  $G_{\mathcal{B}} \cong \langle a, b, c \mid a^2, b^2, c^2 \rangle = C_2 * C_2 * C_2$ .

Information about  $G_{\mathcal{M}}$  as an abstract group can be used to obtain information about the Schreier graphs  $\Gamma_{\mathcal{M},n}$ . See Remarks 11.7 and 11.6.

#### 5. TREES AND AUTOMORPHISMS

In this context it is natural to think of the set of finite words  $A^*$  as vertices in a regular rooted tree, where the empty word is the root and the children of the word  $s$  are the words  $sx$  for  $x \in A$ . We will need to talk about rooted trees more generally, so we make the following definitions.

**Definition 5.1.** A *rooted tree* (or simply *tree*) is a graph  $\mathbf{T}$  with a distinguished root vertex  $r \in \mathbf{T}$  such that for each  $v \in \mathbf{T}$  there is exactly one directed path from  $r$  to  $v$ . The *level* of  $v$ , denoted  $\ell(v)$  is the length of this path. The *n-th level* of  $\mathbf{T}$ , denoted  $\mathbf{T}_n$  is the set of all vertices  $v \in \mathbf{T}$  such that  $\ell(v) = n$ . A *subtree* of  $\mathbf{T}$  is a subgraph containing  $r$  which is itself a rooted tree. A *tree isomorphism* between two trees  $\mathbf{S}$  and  $\mathbf{T}$  is a graph isomorphism which sends the root of  $\mathbf{S}$  to the root of  $\mathbf{T}$ . An *automorphism* of  $\mathbf{T}$  is an isomorphism from  $\mathbf{T}$  to  $\mathbf{T}$ . The automorphisms of  $\mathbf{T}$  form a group, and we denote it  $\text{Aut}(\mathbf{T})$ .

Then, given a Mealy automaton  $\mathcal{M} = (Q, A, \sigma, \tau)$ , for any  $q \in Q$  the map  $\sigma_q : A^* \rightarrow A^*$  is a tree automorphism. That is,  $\sigma_q$  is a bijection which fixes the empty word, and sends children of  $x$  to children of  $\sigma_q(x)$ . In other words, for every  $s \in A^*$  and  $x \in A$  there is some  $y \in A$  such that

$$\sigma_q(sx) = \sigma_q(s)y.$$

Of course, it follows that for any  $w \in Q^*$ , the map  $\sigma_w : A^* \rightarrow A^*$  is a composition of tree automorphisms and is itself a tree automorphism.

Infinite words, i.e., elements of  $A^\infty$ , can be thought of as rays in the tree  $A^*$ , and  $\sigma_w$  acts on them in the natural way.

Note that in order to think of  $\tau_a : Q^* \rightarrow Q^*$  as a tree automorphism, we must think of  $Q^*$  as a tree in the reverse way, i.e. the children of  $w$  are of the form  $qw$  for  $q \in Q$ , rather than of the form  $wq$ .

Given a tree automorphism  $g : A^* \rightarrow A^*$  and a word  $s \in A^*$ , the *section* of  $g$  at  $s$ , is the tree automorphism  $g|_s : A^* \rightarrow A^*$  defined by

$$g(st) = g(s)g|_s(t).$$

Note that we are using a canonical identification between branches of the tree  $A^*$ . There need not be such an identification in a general tree, so this definition of sections is specific to trees of words.

We call a tree automorphism  $\alpha : A^* \rightarrow A^*$  *automatic* if it  $\alpha = \sigma_{\mathcal{M},q}$  for state  $q$  of some Mealy automaton  $\mathcal{M}$ . Equivalently,  $\alpha$  is automatic if and only if it has finitely many sections. The set of automatic automorphisms forms a subgroup  $\text{FAut}(A^*) < \text{Aut}(A^*)$ .

An automorphism  $g : A^* \rightarrow A^*$  is determined by its action on the first level,  $(A^*)_1 = A^1 = A$ , and its sections  $g|_x$  at all  $x \in A$ . If  $\rho : A \rightarrow A$  is a permutation, then for notational convenience we can extend  $\rho$  as an automorphism  $A^* \rightarrow A^*$  via

$$\rho(xs) = \rho(x)s.$$

If  $A$  is equipped with an ordering of its elements, say,  $A = \{x_1, \dots, x_k\}$ , then we write

$$(g_1, \dots, g_k)$$

for the automorphism  $g : A^* \rightarrow A^*$  which acts trivially on  $A$ , and for which  $g|_{x_i} = g_i$  for all  $i$ . Then every automorphism can be uniquely decomposed into

$$g = \rho(g_1, \dots, g_k),$$

for some permutation  $\rho : A \rightarrow A$  and some automorphisms  $g_i : A^* \rightarrow A^*$ . Specifically,  $\rho$  is the restriction of  $g$  to  $A$ , and  $g_i = g|_{x_i}$ . Then, given an invertible Mealy automaton  $\mathcal{M} = (Q, A, \tau, \sigma)$ , the definition of the automorphisms  $\sigma_q$  can be phrased recursively as

$$\sigma_q = \sigma_q(\sigma_{q_1}, \dots, \sigma_{q_k}),$$

where  $q_i = q^{x_i}$ . Such a recursive definition is called a *wreath recursion*. For example, if  $\mathcal{B} = (Q, A, \tau, \sigma)$  is the Bellaterra automaton, then we have the wreath recursion

$$\begin{aligned} \sigma_a &= (\sigma_b, \sigma_c) \\ \sigma_b &= (\sigma_c, \sigma_b) \\ \sigma_c &= \rho(\sigma_a, \sigma_a), \end{aligned}$$

where  $\rho : \{0, 1\} \rightarrow \{0, 1\}$  swaps 0 and 1.

**Definition 5.2.** Let  $\mathbf{T}$  be a rooted tree. We say a tree automorphism  $g : \mathbf{T} \rightarrow \mathbf{T}$  is *spherically transitive* (or just *transitive*) if its restriction to every level of  $\mathbf{T}$  is a transitive map.

For example, if  $\mathcal{M}$  is the adding automaton pictured in Figure 4, then  $\sigma_r : \{0, 1\}^* \rightarrow \{0, 1\}^*$  is spherically transitive, because its action on the  $n$ -th level is addition of 1 modulo  $2^n$ .

## 6. THE BELLATERRA AUTOMATON

Consider the Bellaterra automaton  $\mathcal{B} = (Q, A, \sigma, \tau)$ , pictured in Figure 3. We want to show that the graphs  $B_n = \Gamma_{\mathcal{B},n}$  have small diameter. Our approach is to find short words in  $Q^*$  which change only the last digit of the word  $1^n = 11 \dots 1$ . So, we are looking for words which do not fix the infinite word  $1^\infty = 111 \dots$ , but do preserve the first  $n$  of its letters. It turns out there are enough of these words because  $\tau_1$  acts “transitively enough” on  $Q^*$ , so that almost every orbit under its action contains some word  $w \in Q^*$  which swaps 0 and 1.



It is straightforward to check that  $a^2$ ,  $b^2$ , and  $c^2$  act trivially on  $A^*$ , (i.e.  $\sigma_{aa} = \sigma_{bb} = \sigma_{cc} = \text{id}$ ) so we are primarily interested in *reduced words* in  $\{a, b, c\}$ , i.e. those which do not repeat the same letter twice in a row. Note that these words form a subtree of  $Q^*$ , which is nearly a binary tree: every vertex has two children, except the root.

We will need a simple result on the transitivity of automorphisms of a binary tree.  $A = \{0, 1\}$ . Define a group homomorphism  $\chi : \text{Aut}(A^*) \rightarrow \mathbb{Z}_2[[t]]$ , by

$$\chi(g) = \sum_{n=1}^{\infty} c_n t^{n-1},$$

where  $(-1)^{c_n}$  is the sign of the permutation given by the action of  $\chi$  the  $n$ -th level of  $A^*$ . Values of this homomorphism can be computed recursively via

$$\chi(g) = c_1 + t(\chi(g|_x) + \chi(g|_y)),$$

where  $c_1$  is 0 if  $g$  fixes the two elements of  $A$ , and  $c_1 = 1$  if  $g$  swaps them. We call  $\chi(g)$  the *characteristic function of  $g$* . Of course, this definition makes sense when  $A$  is any two-element set, so we will state the lemma more generally:

**Lemma 6.1.** *Let  $A = \{x, y\}$ . An automorphism  $g \in \text{Aut}(A^*)$  is spherically transitive if and only if  $\chi(g) = 1/(1-t)$ .*

*Proof.* If  $g$  is spherically transitive, then its action on the  $n$ -th level of  $A^n$  is a  $(2^n)$ -cycle, which is an odd permutation for all  $n \geq 1$ . Hence,  $c_n = 1$  for all  $n \geq 1$ , and

$$\chi(g) = \sum_{n=1}^{\infty} t^{n-1} = \frac{1}{1-t}.$$

In the other direction, suppose  $\chi(g) = 1/(1-t)$ , i.e.  $g$  acts as an odd permutation on  $A^n$  for every  $n \geq 1$ . We will show by induction on  $n$  that the action of  $g$  on  $A^n$  is a  $(2^n)$ -cycle for all  $n \geq 0$ . This is trivial for  $n = 0$ .

For the inductive step, suppose  $g$  acts as a  $(2^n)$ -cycle on  $A^n$ . Given a word  $s \in A^n$ , we either have  $g^{2^n}(sx) = sx$  or  $g^{2^n}(sx) = sy$ . In the first case  $sx$  belongs to a  $(2^n)$ -cycle of  $g$ , in the second case,  $sx$  belongs to a  $(2^{n+1})$ -cycle. So, any word in  $A^{n+1}$  ending in  $x$  belongs to either a  $(2^n)$ -cycle or a  $(2^{n+1})$ -cycle, and similarly for words ending in  $y$ . So, the action of  $g$  on  $A^{n+1}$  decomposes into either two  $(2^n)$ -cycles or a single  $(2^{n+1})$ -cycle. But the former is an even permutation, so  $g$  must act as a  $(2^{n+1})$ -cycle on  $A^{n+1}$ , as desired.  $\square$

**Lemma 6.2.** *Let  $\mathcal{B} = (Q, A, \tau, \sigma)$  denote the Bellaterra automaton. Then for every natural number  $n$ , the map  $\tau_{\mathcal{B},1}$  acts transitively on the set of reduced words of length  $n$  ending with  $a$  or  $c$ .*

*Proof.* We will write the argument down in terms of the dual automaton  $\overline{\mathcal{B}} = (A, Q, \overline{\tau}, \overline{\sigma})$ , pictured in Figure 3. Since taking the dual reverses words, we want to show that  $\sigma_1 = \sigma_{\overline{\mathcal{B}},1}$  acts transitively on the binary subtree  $\mathbf{T} \subset Q^*$  of reduced words which *begin* with  $a$  or  $c$ .

It is convenient to put  $\mathbf{T}$  into bijection with a binary tree of words  $\mathbf{R} = \{\uparrow, \downarrow\}^*$ . We define the maps  $\phi_a, \phi_b, \phi_c : \mathbf{R} \rightarrow Q^*$  recursively by

$$\begin{aligned} \phi_a(\uparrow w) &= b\phi_b(w) & \phi_a(\downarrow w) &= c\phi_c(w) \\ \phi_b(\uparrow w) &= c\phi_c(w) & \phi_b(\downarrow w) &= a\phi_a(w) \\ \phi_c(\uparrow w) &= a\phi_a(w) & \phi_c(\downarrow w) &= b\phi_b(w) \end{aligned}$$

It is straightforward to check by induction on word length that for each  $x \in Q$ ,  $\phi_x$  defines a tree isomorphism between  $\mathbf{R}$  and the reduced words in  $Q^*$  which do not begin with  $x$ . In particular,  $\phi_b$  is a bijection between  $\mathbf{R}$  and  $\mathbf{T}$ .

Now consider the dual  $\overline{\mathcal{B}}$  of the Bellaterra automaton, and in particular the corresponding automorphisms  $\sigma_0, \sigma_1 \in \text{Aut}(Q^*)$ . Given  $x, y \in Q$ ,  $d \in A$ , define

$$\sigma_{x,d,y} = \phi_x^{-1} \sigma_d \phi_y \in \text{Aut}(\mathbf{R}).$$

Note that, a priori, the domain of  $\phi_x^{-1}$  may not coincide with the image of  $\sigma_d\phi_y$ , so  $\sigma_{x,d,y}$  may be ill-defined for some values of  $x, d, y$ . However, the computations below give an explicit recursion for computing  $\sigma_{1,b,1}$ , which also demonstrates that it is well-defined.

We can compute that, e.g.,

$$\begin{aligned}\sigma_{b,1,b}(\uparrow w) &= \phi_b^{-1}(\sigma_1(\phi_b(\uparrow w))) \\ &= \phi_b^{-1}(\sigma_1(c\phi_c(w))) \\ &= \phi_b^{-1}(a\sigma_0(\phi_c(w))) \\ &= \downarrow\phi_a^{-1}(\sigma_0(\phi_c(w))) \\ &= \downarrow\sigma_{a,0,c}\end{aligned}$$

In particular,  $\sigma_{b,1,b}|_{\uparrow} = \sigma_{a,0,c}$ .

Similar computations give the complete recursive description of  $\sigma_{b,1,b}$ , which we write down using the usual wreath recursion notation  $g = \rho^\varepsilon(g|_{\uparrow}, g|_{\downarrow})$ , where  $\rho$  swaps  $\uparrow$  and  $\downarrow$ :

$$\begin{aligned}\sigma_{b,1,b} &= \rho(\sigma_{a,0,c}, \sigma_{c,1,a}) \\ \sigma_{a,0,c} &= (\sigma_{b,0,a}, \sigma_{c,0,b}) \\ \sigma_{c,1,a} &= \rho(\sigma_{b,1,b}, \sigma_{a,0,c}) \\ \sigma_{b,0,a} &= (\sigma_{c,0,b}, \sigma_{a,1,c}) \\ \sigma_{c,0,b} &= (\sigma_{a,1,c}, \sigma_{b,0,a}) \\ \sigma_{a,1,c} &= \rho(\sigma_{c,1,a}, \sigma_{b,1,b})\end{aligned}$$

Defining  $F_{x,d,y} = \chi(\sigma_{x,d,y})$ , this gives us the following linear equations in the ring  $\mathbb{Z}_2[[t]]$ :

$$\begin{aligned}F_{b,1,b} &= 1 + t(F_{a,0,c} + F_{c,1,a}) \\ F_{a,0,c} &= t(F_{b,0,a} + F_{c,0,b}) \\ F_{c,1,a} &= 1 + t(F_{b,1,b} + F_{a,0,c}) \\ F_{b,0,a} &= t(F_{c,0,b} + F_{a,1,c}) \\ F_{c,0,b} &= t(F_{a,1,c} + F_{b,0,a}) \\ F_{a,1,c} &= 1 + t(F_{c,1,a} + F_{b,1,b})\end{aligned}$$

Solving this system of equations yields

$$\begin{aligned}F_{b,1,b} &= 1/(1-t) \\ F_{a,0,c} &= 0 \\ F_{c,1,a} &= 1/(1-t) \\ F_{b,0,a} &= t/(1-t) \\ F_{c,0,b} &= t/(1-t) \\ F_{a,1,c} &= 1,\end{aligned}$$

So we have

$$\chi(\phi_b^{-1}\sigma_{\overline{B},1}\phi_b) = 1/(1-t).$$

By Lemma 6.1, the automorphism  $\phi_b^{-1}\sigma_1\phi_b$  acts transitively on  $\mathbf{R}$ . Hence  $\sigma_1$  acts transitively on  $\mathbf{T}$ , that is, for each  $n$  it acts transitively on the set of length  $n$  reduced words in  $\{a, b, c\}$  which begin with  $a$  or  $c$ . Hence, in the unreversed Bellaterra automaton  $\mathcal{B}$ , we have that  $\tau_{\mathcal{B},1}$  acts transitively on the words of a given length which end with  $a$  or  $c$ .  $\square$

**Lemma 6.3.** *Let  $\mathcal{M} = (Q, A, \tau, \sigma)$  be a Mealy automaton, let  $x$  be a letter in  $A$ , and let  $w$  be a word in  $Q^*$ . Then  $w$  stabilizes the infinite word  $xxx\dots = x^\infty$  if and only if every element of the*

orbit of  $w$  under  $\tau_x$  stabilizes  $x$ . That is,

$${}^w(xx\ldots) = xx\ldots \quad \text{if and only if} \quad \sigma(\tau_x^n(w), x) = x \text{ for all } n \geq 0.$$

*Proof.* Say

$${}^w(xx\ldots) = y_0y_1y_2\ldots$$

Then  $y_n$  is the last letter of  ${}^w(x^{n+1})$ . Letting  $X = x^n$ , we have

$${}^w(x^{n+1}) = {}^w(Xx) = {}^w(X) \tau^{(w,X)}x,$$

So,

$$y_n = \tau^{(w,X)}x = \sigma(\tau(w, X), x) = \sigma(\tau_X(w), x) = \sigma(\tau_x^n(w), x),$$

and therefore  ${}^wxx\ldots = xx\ldots$  if and only if  $\sigma(\tau_x^n(w), x) = x$  for every  $n \geq 0$ , as desired.  $\square$

**Theorem 6.4.** *Let  $B_n$  denote the  $n$ -th Bellaterra graph. Then  $\text{diam}(B_n) = O(n^2)$ .*

*Proof.* Let  $\mathcal{B} = (Q, A, \tau, \sigma)$  denote the Bellaterra automaton, so that  $B_n = \Gamma_{\mathcal{B}, n}$ . It is enough to show that for some  $C$  the ball of radius  $Cn^2$  around the vertex  $1^n = 11\ldots 1$  covers all of  $B_n$ . That is, we will show that for every number  $n$ , and every  $v \in B_n$ ,

$$d(1^n, v) \leq Cn^2.$$

The only letter in  $Q = \{a, b, c\}$  which swaps the elements of  $A$  is  $c$ . The other two letters fix 0 and 1. Hence, a word  $w \in Q^*$  fixes 1 if and only if it has an even number of  $c$ 's.

For each  $n > 0$ , there is a reduced word ending in  $a$  or  $c$  which contains an odd number of  $c$ 's. We can take, e.g.  $abab\ldots abc$  or  $baba\ldots abc$ . By Lemma 6.2, if  $w$  is any reduced word of length  $n$  ending in  $a$  or  $c$ , then its orbit under  $\tau_1$  contains some word which does not fix 1. Hence, by Lemma 6.3,  $w$  does not fix the infinite word  $111\ldots = x^\infty$ .

Given a number  $n \geq 1$ , we have  $|A^n| = 2^n$ , and there are  $2^{n+1} - 1$  reduced words of length  $n$  or less which end in  $a$  or  $c$ . By the pigeonhole principle, there must be two such words,  $v, w$  with  $v(1^n) = w(1^n)$ . We may assume  $\ell(v) \leq \ell(w)$ . Since  $a^2$ ,  $b^2$ , and  $c^2$  all act trivially on  $A^*$ , reversing a word inverts its action on  $A^*$ . Let  $u$  be the reduced word formed by cancelling pairs of repeated letters in  $\bar{v}w$ . Then,

$$u(1^n) = \bar{v}w(1^n) = \bar{v}(1^n) = 1^n,$$

$$\text{and } \ell(u) \leq \ell(\bar{v}w) = \ell(v) + \ell(w) \leq 2n.$$

Since  $v \neq w$ ,  $u$  is not the empty word. We assumed that  $\ell(v) \leq \ell(w)$ , so the last letter of  $w$  is not cancelled. Hence  $u$  also ends in  $a$  or  $c$ , and therefore

$$u(111\ldots) \neq 111\ldots$$

Let  $k$  be the maximal integer such that  $u(1^k) = 1^k$ . We know  $k \geq n$  and  $u(1^{k+1}) = 1^k 0$ . So, letting  $s = 1^{k-n}$ ,  $t = 1^{n+1}$ , and  $t' = 1^n 0$ , we have

$$st' = u(st) = u_s u'(t) = s u'(t),$$

where  $u' = u^s$ . So we have

$$u'(1^{n+1}) = 1^n 0,$$

$$\text{and } \ell(u') = \ell(u) \leq 2n.$$

This construction works for all  $n \geq 1$ . That is, for every  $n \geq 1$ , there exists a  $u_n \in Q^*$  with  $\ell(u_n) \leq 2n$  and  $u_n(1^n 0) = 1^{n+1}$ .

We now prove by induction on  $n$  that for every  $s \in A^n$ , there is a  $w \in Q^*$  with  $\ell(w) \leq n^2$  such that  ${}^ws = 1^n$ . The base cases  $n = 0$  and  $n = 1$  are trivial. For the inductive step, consider any  $n \geq 1$ . Given  $s \in A^{n+1}$ , let  $s'$  be  $s$  with the last digit removed. By the induction hypothesis know there is a word  $w$  with  $\ell(w) \leq n^2$  such that  ${}^ws' = 1^n$ . Then either  ${}^ws = 1^{n+1}$  or  ${}^ws = 1^n 0$ . In the

first case, we are done. In the second case,  $u_n w s = 1^{n+1}$ , and  $\ell(u_n w) \leq 2n + n^2 \leq (n+1)^2$ , so we are done.

So, we have shown that in the graph  $B_n = \Gamma_{\mathcal{B},n}$ , we have  $d(1^n, s) \leq n^2$  for every  $s \in A^n$ . It follows that for any  $s, t \in B_n$ ,

$$d(s, t) \leq d(s, 1^n) + d(1^n, t) \leq 2n^2,$$

i.e.  $\text{diam}(B_n) \leq 2n^2$ . □

## 7. THE ALESHIN AUTOMATON

The Aleshin automaton  $\mathcal{A}$  and the Bellaterra automaton  $\mathcal{B}$  are closely related. Indeed, let  $\tau_d : \{0, 1\}^* \rightarrow \{0, 1\}^*$  denote map which swaps every digit of a binary word. Then it is straightforward to check by induction that

$$\begin{aligned} \tau_{\mathcal{A},a} &= \tau_d \tau_{\mathcal{B},a}, \\ \tau_{\mathcal{A},b} &= \tau_d \tau_{\mathcal{B},c}, \\ \text{and } \tau_{\mathcal{A},c} &= \tau_d \tau_{\mathcal{B},b}. \end{aligned}$$

With this observation, Theorem 6.4 has the following corollary.

**Corollary 7.1.** *Let  $A_n$  denote the  $n$ -th Aleshin graph. Then  $\text{diam}(A_n) = O(n^2)$ .*

*Proof.* For every pair  $q, r \in \{a, b, c\}$ , we have

$$\tau_{\mathcal{A},q}^{-1} \tau_{\mathcal{A},r} = \tau_{\mathcal{B},q}^{-1} \tau_d^{-1} \tau_d \tau_{\mathcal{B},r} = \tau_{\mathcal{B},q} \tau_{\mathcal{B},r}.$$

So, if two words in  $\{0, 1\}^n$  are separated by a path of length 2 in the Bellaterra graph  $B_n$ , they are also separated by a path of length 2 in the Aleshin graph  $A_n$ . It follows that two endpoints of an even-length path in  $B_n$  are endpoints of a path in  $A_n$  of the same length.

For any word  $s \in \{0, 1\}^n$  there is a path in  $B_n$  of length  $O(n^2)$  from  $1^n$  to  $s$ . We may assume that this path has even length since  $1^n$  has an edge in  $B_n$  from itself to itself. This corresponds to a path in  $A_n$  of the same length, so for any  $s \in \{0, 1\}^n$ , there is a path in  $A_n$  of length  $O(n^2)$  from  $1^n$  to  $s$ . Therefore,  $\text{diam}(\Gamma_{\mathcal{A},n}) = O(n^2)$ , as desired. □

## 8. GENERALIZATIONS

The proof of Theorem 6.4 can be adapted to prove a more general result. In order to generalize to automata with larger alphabets, we need to consider a restricted type of automaton. We say an Mealy automaton  $\mathcal{M} = (Q, A, \tau, \sigma)$  is *cyclic* if it is invertible, and  $\langle \sigma_q \mid q \in Q \rangle = \langle (x_1 x_2 \dots x_n) \rangle$ , where  $\{x_1, x_2, \dots, x_n\} = A$ . That is, if its action on  $A$  is a cyclic permutation group. In particular, any automaton with  $|A| = 2$  is cyclic. This will enable us to reach any word of the form  $x^n y$  from  $x^{n+1}$  in a short time, as long as we can reach some such word.

We first state and prove the general result with the weakest assumptions under which our argument guarantees polynomial growth of  $\text{diam}(\Gamma_{\mathcal{M},n})$ .

**Theorem 8.1.** *Let  $\mathcal{M} = (Q, A, \sigma, \tau)$  be a cyclic Mealy automaton with  $|A|$  prime, and let  $\Gamma = \Gamma_{\mathcal{M},\infty}$ . Suppose there is a letter  $x \in A$  and constants  $\alpha > 0$ ,  $K > 1$  such that, for sufficiently large  $r$ ,*

$$|B_\Gamma(xxx\dots, r)| \geq K^{r^\alpha}.$$

*Then there is a constant  $C > 0$ , such that for all  $n$ ,*

$$\text{diam}(\Gamma_{\mathcal{M},n}) \leq Cn^{1+1/\alpha}.$$

*Proof.* Let  $p = |A|$ . By replacing  $\mathcal{M}$  with  $\mathcal{M} \cup \mathcal{M}^{-1}$  if necessary, we may assume that for every  $q \in Q$ , there is a  $q' \in Q$  with  $\sigma_{q'} = \sigma_q^{-1}$ . This replacement adds edges to the Schreier graphs  $\Gamma_{\mathcal{M},n}$ , but only reverses of edges which were already there, so  $\text{diam}(\Gamma_{\mathcal{M},n})$  and  $B_{\Gamma_{\mathcal{M},n}}(s, r)$  are unaffected. Then for a word  $w \in Q^*$ , we define  $w^{-1}$  to be  $w$ , reversed, with each letter  $q$  replaced by  $q'$ , so that  $\sigma_{w^{-1}} = \sigma_w^{-1}$ .

Given sufficiently large  $n$ , pick  $r$  such that

$$((\log_K p)n)^{1/\alpha} < r < 2((\log_K p)n)^{1/\alpha}.$$

Then  $|B_\Gamma(xxx \dots, r)| > p^n$ . By the pigeonhole principle, some two elements of  $B_\Gamma(xxx \dots, r)$  have the same first  $n$  digits. That is, there are  $v, w \in (Q \cup Q^{-1})^*$  with

$$\ell(v), \ell(w) \leq r, \quad v(x^n) = w(x^n), \quad \text{and} \quad v(xxx \dots) \neq w(xxx \dots).$$

So, there is a  $u_0 = v^{-1}w \in (Q \cup Q^{-1})^*$  with

$$\begin{aligned} \ell(u_0) &\leq 2r, \\ u_0(x^n) &= x^n, \\ \text{and} \quad u_0(xxx \dots) &\neq xxx \dots \end{aligned}$$

There is some smallest value of  $k \geq n+1$  such that  $u_0(x^k) \neq x^k$ . Let  $X_0 = x^{k-n-1}$  and  $X = x^n$ , so that  $x^k = X_0 X x$  and  $u_0(x^k) = X_0 X y$  for some  $y \in A$  with  $y \neq x$ . Let  $u = u_0^{X_0}$  so in particular,  $\ell(u) = \ell(u_0)$ . Then,

$$X_0 X y = u_0(X_0 X x) = u_0 X_0 u(Xx) = X_0 u(Xx),$$

so

$$u(Xx) = Xy.$$

Similarly, if  $u' = u^X$ , we have

$$u(Xz) = X u' z$$

for any  $z \in A$ . Since  $u' x = y \neq x$  and  $\mathcal{M}$  is cyclic, the action of  $u'$  on  $A$  is a nontrivial cyclic permutation. Since  $p = |A|$  is prime,  $u'$  acts transitively on  $A$ , and therefore  $u$  acts transitively on  $\{Xz \mid z \in Aa\}$ . It follows that for any  $z, z' \in A$ ,

$$d(Xz, Xz') \leq p \ell(u) \leq 2pr \leq 4p((\log_K p)n)^{1/\alpha}.$$

Thus, there is a constant  $C$  such that for sufficiently large  $n$ , we have

$$d(x^n z, x^{n+1}) \leq Cn^{1/\alpha}, \quad \text{for all } z \in A.$$

By increasing the constant if necessary, we can make this true for all  $n$ .

Now let us show by induction on  $n$  that for all  $s \in A^n$ , we have  $d(s, x^n) < Cn^{1+1/\alpha}$ . The base case  $n = 0$  is trivial. For the inductive step, take any  $s \in A^{n+1}$ , and let  $s'$  be its first  $n$  letters. We know  $d(s', x^n) < Cn^{1+1/\alpha}$ . There is some word  $w \in (Q \cup Q^{-1})^*$  with  $\ell(w) = d(s', x^n)$  and  $w(s') = x^n$ . Then  $ws = x^n z$  for some  $z \in B$ . Thus,

$$\begin{aligned} d(s, x^{n+1}) &\leq d(s, x^n z) + d(x^n z, x^{n+1}) \\ &\leq Cn^{1+1/\alpha} + Cn^{1/\alpha} \\ &\leq C(n+1)^{1+1/\alpha}, \end{aligned}$$

which completes the induction.

It follows that for any  $s, t \in A^n$ ,  $d(s, t) \leq d(s, x^n) + d(x^n, t) \leq 2Cn^{1+1/\alpha}$ , i.e.,

$$\text{diam}(\Gamma_{\mathcal{M},n}) \leq 2Cn^{1+1/\alpha}.$$

□

In all the cases where we apply this,  $|B_\Gamma(xxx\dots, r)|$  will have exponential growth, so we state that case separately.

**Corollary 8.2.** *Let  $\mathcal{M} = (Q, A, \sigma, \tau)$  be a cyclic Mealy automaton with  $|A|$  prime. Let  $\Gamma = \Gamma_{\mathcal{M}, \infty}$ . If there is an  $x \in A$  and a constant  $K > 1$  such that*

$$|B_\Gamma(xxx\dots, r)| \geq K^r$$

*for sufficiently large  $r$ , then there is a constant  $C > 0$ , such that*

$$\text{diam}(\Gamma_{\mathcal{M}, n}) \leq Cn^2.$$

It is not always easy to guarantee that  $|B_\Gamma(xxx\dots, r)| \geq K^r$  grows quickly, so we prove an additional result based on the size of orbits of  $\tau_x$  in  $Q^n$ . Loosely, if the orbits grow quickly enough, it must be because there are enough distinct images of words of the form  $x^m$ .

**Theorem 8.3.** *Let  $\mathcal{M} = (Q, A, \sigma, \tau)$  be a reversible<sup>3</sup> cyclic Mealy automaton with  $|A|$  prime. Suppose there is a letter  $x \in A$  and constants  $K > 1$ ,  $\alpha > 0$  such that for sufficiently large  $n$ , there is a  $w \in Q^n$  with*

$$|\{\tau_x^k(w) \mid k \in \mathbb{Z}\}| \geq K^{n^\alpha}.$$

*Then there is a constant  $C > 0$ , such that for all  $n$ , we have*

$$\text{diam}(\Gamma_{\mathcal{M}, n}) \leq Cn^{1+1/\alpha}.$$

*Proof.* Let  $P = \{p \in \mathbb{N} \mid p \text{ prime}, p \leq |Q|\}$ . It is easy to see by induction on length that for each  $w \in Q^*$ , the sequence  $w, \tau_x(w), \tau_x^2(w), \dots$  is periodic with period  $m$ , where  $m$  is a product of some powers of primes in  $P$ . Define letters  $q_{i,k}$  via

$$\tau_x^k(w) = q_{0,k}q_{1,k}\dots q_{n,k}.$$

If  $m_i$  is the period of the sequence  $q_{i,0}, q_{i,1}, \dots$ , then  $m = \gcd(m_0, m_1, \dots, m_n)$ . Let  $M = \max_i m_i$ . Then each prime power in the prime factorization of  $m$  is a factor of some  $m_i$ , so it is at most  $M$ . The period  $m$  is the product of these prime powers, so  $m \leq M^{|P|}$ . That is, there is some  $i$  such that  $m_i \geq m^{1/|P|}$ .

Fix that  $i$  for the rest of the proof, and let  $v$  be the first  $i$  letters of  $w$ . Consider the infinite word  $s = {}^v(xxx\dots)$ , and let  $x_k$  be it's  $k$ -th letter. Let  $l$  be the period of the word  $s$ . Note that  $q_{i,k+1} = q_{i,k}^{x_k}$  and therefore

$$q_{i,k+l} = q_{i,k}^X,$$

where

$$X = x_k x_{k+1} \dots x_{k+l-1}.$$

Since the  $x_k$  repeat every  $l$  letters, we have  $q_{i,k+l} = q_{i,k}^X$ , and  $q_{i,k+2l} = q_{i,k+l}^X$ , and so on. Let  $F = |Q|!$ . Then  $X^F$  acts trivially on  $Q$ , and hence  $q_{i,k+Fl} = q_{i,k}^{X^F}$ . This is true for each  $k$ , so the  $q_{i,k}$  have period  $m_i \leq Fl$ . Thus, the word  $s = {}^v(xxx\dots)$  has period  $l \geq m^{1/|P|}/F$ .

Now let  $n$  be sufficiently large, so that there is a word  $w \in Q^n$  whose orbit under  $\tau_x$  has size  $m \geq K^{n^\alpha}$ . Then, from the above, for some  $v \in Q^*$  with  $\ell(v) \leq n$ , the word  $s = {}^v(xxx\dots)$  has period

$$l \geq \frac{1}{F} K^{n^\alpha/|P|} \geq \tilde{K}^{n^\alpha},$$

where we fix some  $1 < \tilde{K} < K^{1/|P|}$ , and the last inequality holds for sufficiently large  $n$ .

Let  $v_k = \tau_x^k(v)$ . Then  ${}^{v_k}xxx\dots$  is a shift of  $s$ , and since  $s$  has period  $l$  there are  $l$  distinct such shifts. So, since each  $v_k$  satisfies  $\ell(v_k) \leq n$ , the set  $\{{}^{v_k}xxx\dots \mid w \in Q^*, \ell(w) \leq n\}$  has at least  $l \geq \tilde{K}^{n^\alpha}$  elements. It follows that  $|B_\Gamma(xxx\dots, n)| \geq \tilde{K}^{n^\alpha}$ , where  $\Gamma = \Gamma_{\mathcal{M}, \infty}$ .

So Theorem 8.1 applies, and there is a constant  $C$  such that  $\text{diam}(\Gamma_{\mathcal{M}, n}) \leq Cn^{1+1/\alpha}$ .  $\square$

<sup>3</sup>The assumption that  $\mathcal{M}$  is reversible may be lifted, if we replace  $|\{\tau_x^k(w) \mid k \in \mathbb{Z}\}|$  with the length of the (eventual) period of  $w, \tau_x(w), \tau_x^2(w), \dots$ .

We also state the following special case, which is a simple way to apply the theorem.

**Corollary 8.4.** *Let  $\mathcal{M} = (Q, A, \sigma, \tau)$  be a reversible cyclic Mealy automaton with  $|A|$  prime. Suppose there is some  $a \in A$ , and some  $d \geq 2$ , such that there is a  $d$ -regular subtree  $\mathbf{T} \subseteq Q^*$  such that  $\tau_a$  acts spherically transitively on  $\mathbf{T}$ . Then there is a constant  $C > 0$ , such that for all  $n$ , we have*

$$\text{diam}(\Gamma_{\mathcal{M},n}) \leq Cn^2.$$

## 9. COTRANSITIVE CYCLIC AUTOMATA

The simplest way for the conditions in Corollary 8.4 to be satisfied is when some  $\tau_a$  acts spherically transitively on the entire tree  $Q^*$ . With that in mind, we make the following definitions.

We say an invertible Mealy automaton  $\mathcal{M} = (Q, A, \sigma, \tau)$  is  $q$ -transitive if the tree automorphism  $\sigma_q : A^* \rightarrow A^*$  is spherically transitive. We say  $\mathcal{M}$  is *transitive*<sup>4</sup> if it is  $q$ -transitive for some  $q \in Q$ . We say  $\mathcal{M}$  is *cotransitive* if its dual is transitive.

Then, according to Corollary 8.4, we have

**Corollary 9.1.** *Let  $\mathcal{M} = (Q, A, \sigma, \tau)$  be a reversible cyclic cotransitive Mealy automaton with  $|A|$  prime. Then  $\text{diam}(\Gamma_{\mathcal{M},n}) = O(n^2)$ .*

We do not know a general method for determining whether a tree automorphism given by an automaton is transitive, but there are special cases where checking it is easier. For example, [St] gives a generalization of Lemma 6.1 to all cyclic automata:

**Lemma 9.2.** *Let  $\mathcal{M} = (Q, A, \tau, \sigma)$  be a cyclic automaton, with  $|A| = m$ . Then there is a cyclic permutation  $\rho$  of  $A$ , such that for each  $q \in Q$  there is a  $k_q$  s.t.  $\sigma_q = \rho^{k_q}$ . Recursively define*

$$\chi(q) = k_q + t \sum_{x \in A} \chi(\tau_x(q)) \in \mathbb{Z}_m[[t]]$$

*Then  $\sigma_q$  acts transitively on  $A^*$  if and only if each coefficient of  $\chi(q)$  is a generator of  $\mathbb{Z}_m$ .*

An automaton is called *cocyclic* if its dual is cyclic. Now observe that the power series  $\chi(q)$  for  $q \in Q$  satisfy a recursive linear relation, which can be solved to write each  $\chi(q)$  as a rational function. This implies:

**Corollary 9.3.** *Given a (co)cyclic Mealy automaton  $\mathcal{M} = (Q, A, \tau, \sigma)$ , there is an algorithm to determine whether it is (co)transitive.*

For example, it is straightforward to check that, there are 16 cocyclic invertible  $(3, 2)$ -automata, and only four are cotransitive. These four are the automata pictured in Figures 6b–6e, i.e., automata number 956, 2396, 870, and 2294 in [B+].<sup>5</sup>

## 10. FURTHER EXAMPLES

**Example 10.1.** It can be verified that, except for the automata pictured in Figure 6, every invertible  $(3, 2)$ -automaton is not cotransitive: for each automaton, simply find orbits of each  $\tau_a$  which are proper subsets of  $A^n$  for some  $n$ . In this case, it suffices to take  $n = 4$ .

The final automaton  $\mathcal{M}$  pictured in Figure 6a, which is automaton number 2372 in [B+], is not cocyclic. So, we do not have a mechanical procedure to prove it is cotransitive. It turns out, however, that there is an automorphism  $\kappa : \{a, b, c\}^* \rightarrow \{a, b, c\}^*$  such that  $\kappa^{-1}\tau_{\mathcal{M},1}\kappa$  can be computed by a cyclic automaton. Indeed, one can take  $\kappa = \tau_{\mathcal{C},x}$ , where  $\mathcal{C}$  is the automaton in Figure 7. Then we can compute the power series  $\chi(\kappa^{-1}\tau_{\mathcal{M},1}\kappa)$ , and see directly that its coefficients are nonzero. At that point, Corollary 9.2 implies that  $\kappa^{-1}\tau_{\mathcal{M},1}\kappa$  acts transitively on  $Q^*$ , and hence so does  $\tau_{\mathcal{M},1}$ .

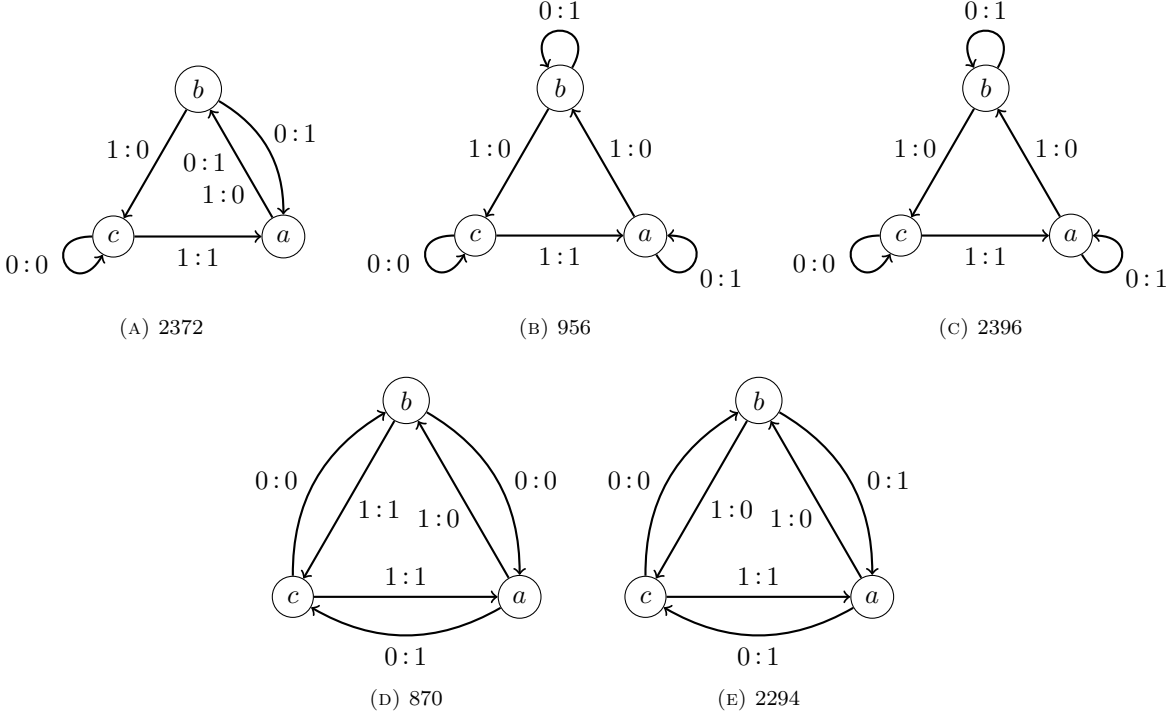
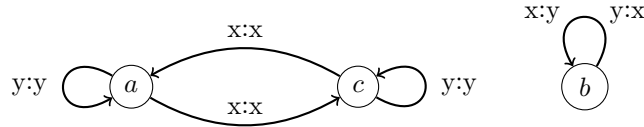


FIGURE 6. The five contrasitive 3-state automata on a binary alphabet.

FIGURE 7. An automaton to conjugate  $\mathcal{M}_{2372}$  into a cocyclic automaton.

So, we have sketched a proof of the following:

**Proposition 10.2.** *The cotransitive invertible  $(3, 2)$ -automata are precisely the five automata pictured in Figure 6, up to relabeling of  $A$  and  $Q$ .*

**Example 10.3.** Of course, there are automata which are not cotransitive, but still satisfy the conditions of Corollary 8.4. As we saw, one example is the Bellaterra automaton. A natural and easy to analyze example is the automaton  $\mathcal{M} = (Q, A, \tau, \sigma)$  that implements division by 3 modulo  $2^n$ . (This is automaton number 924 in [B+]. See [BS] for more on this construction and related ones.) We will also see that its Schreier graphs do not form a family of expanders.

A quick way to define this automaton is that for  $a, b \in Q = \{0, 1, 2\}$  and  $x, y \in A = \{0, 1\}$ , we have  $a \xrightarrow{x:y} b$  if and only if

$$a + 3y = x + 2b.$$

This automaton is pictured in Figure 8. Note that for convenience we abuse notation slightly and call two of the states, 0 and 1, by the same name as the letters in the alphabet.

<sup>4</sup>A more natural definition of this term might be that the  $\sigma_q$  together act transitively on each level of  $A^*$ , but that is too general for our purposes

<sup>5</sup>Note that [B+] does not distinguish between an automaton and its inverse. We do, so some of our automata are actually inverses of the automata described there.



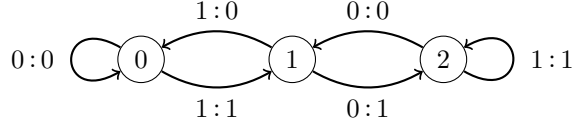


FIGURE 8

By assumption, if  $a \xrightarrow{x:y} b$ , then for any  $x' \in \mathbb{Z}/2^{n-1}\mathbb{Z}$ , we have the following equalities in  $\mathbb{Z}/2^n\mathbb{Z}$ :

$$\begin{aligned} x + 2b &= a + 3y \\ x + 2x' - a &= 3y + 2x' - 2b \\ \frac{(x + 2x') - a}{3} &= y + 2\frac{x' - b}{3}. \end{aligned}$$

That is, if  $x$  is the least significant binary digit of a number  $X \in \mathbb{Z}/2^n\mathbb{Z}$ , and  $x' \in \mathbb{Z}/2^{n-1}\mathbb{Z}$  is the number corresponding to the rest of its digits, then the least significant digit of  $(X - a)/3$  is  $y$ , and the rest of the digits are given by  $(x' - b)/3$ . It follows that if we identify a number  $x \in \mathbb{Z}/2^n\mathbb{Z}$  with its binary representation in  $\{0, 1\}^n$  (with the least significant digit on the left), then we have, for each  $a \in \{0, 1, 2\}$ ,

$$\sigma_a(x) = \frac{x - a}{3}.$$

By a symmetric argument, the dual of this automaton implements division by 2 modulo 3. Phrasing this in terms of the original automaton  $\mathcal{M}$ , we interpret a length- $m$  word in  $\{0, 1, 2\}$  as the representation of a number modulo  $3^m$  written in ternary with the least significant digit on the right. Then for each  $x \in \{0, 1\}$ ,

$$\tau_x(a) = \frac{a - x}{2}.$$

In particular,  $\tau_0$  divides a number by 2. Since 2 generates the multiplicative group  $(\mathbb{Z}/3^m\mathbb{Z})^*$ , that group is an orbit of  $\tau_0$ . So for every  $m$ , there is an orbit of  $\tau_0$  in  $Q^m$  of size  $2 \cdot 3^{m-1}$ . By Theorem 8.3, it follows that  $\text{diam}(\Gamma_{\mathcal{M},n}) = O(n^2)$ . In fact, it can be checked explicitly that  $\text{diam}(\Gamma_{\mathcal{M},n}) = O(n)$ . This can be seen from the observation that the sequence of applications of  $\sigma_1, \sigma_2$ , and  $\sigma_3$  necessary to send the binary number  $x$  to  $00 \dots 0$  is essentially the representation of  $x$  in base 3.

However, the group  $G_{\mathcal{M}} = \langle \sigma_0, \sigma_1, \sigma_2 \rangle$  is generated by  $\mu = \sigma_0^{-1}$  and  $\alpha = \sigma_1^{-1}\sigma_0$ , which are multiplication by 3 and addition of 1, respectively. E.g.,  $\sigma_2 = \mu^{-1}\alpha^{-2}$ . It follows that the group action factors through the group of upper-triangular 2 by 2 matrices via

$$\mu \mapsto \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \quad \alpha \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

This group is solvable, and therefore amenable. It follows that its Schreier graphs with respect to a fixed set of generators cannot be expanders [Lub, 3.3.7]. So, the family  $\{\Gamma_{\mathcal{M},n}\}_{n=1}^{\infty}$  is not a family of expanders.

So, there are automata to which our general results apply, but whose Schreier graphs do not form a family of expanders. More work is necessary to find sufficient conditions for when an automaton gives rise to a family of expanders.

**Example 10.4.** It can be checked by a computation that there are no cotransitive invertible  $(4, 2)$ -automata. It turns out it is enough to check the actions of the  $\tau_a$  on  $Q^4$ .

**Example 10.5.** There are seven  $(5, 2)$ -automata which are not cocyclic, but act transitively on  $Q^{10}$ . Of these, just one is bireversible, as the Aleshin and Bellaterra automata are. It is pictured in

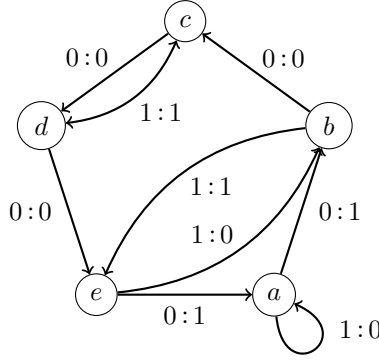


FIGURE 9. The only candidate to be a cotransitive bireversible  $(5, 2)$ -automaton.

Figure 9. Unlike the automaton in Figure 6a, it is unlikely that there is an automatic automorphism  $\kappa : Q^* \rightarrow Q^*$  such that  $\kappa^{-1}\tau_0\kappa$  is implemented by a cocyclic automaton. We have checked that if there is such a  $\kappa$ , the automaton implementing it would need to have at least 48668 states.

## 11. REMARKS AND FURTHER WORK

11.1. The results in Section 8 can be extended to non-invertible Mealy automata as well. Since we are primarily interested only in regular graphs, we prove only the simpler case. For example, to state Theorem 8.1 more generally, one needs to consider the size of balls in  $\Gamma_{\mathcal{M}, \infty}$  defined in terms of directed paths, but the result about the diameter of  $\Gamma_{\mathcal{M}, n}$  still needs diameter to be defined in terms of undirected paths.

11.2. As noted in the proof of Corollary 7.1, any product of two generators of the Bellaterra group  $G_{\mathcal{B}} = \langle \sigma_{\mathcal{B}, a}, \sigma_{\mathcal{B}, b}, \sigma_{\mathcal{B}, c} \rangle$  belongs to the Aleshin group  $G_{\mathcal{A}} = \langle \sigma_{\mathcal{A}, a}, \sigma_{\mathcal{A}, b}, \sigma_{\mathcal{A}, c} \rangle$ . We used this fact to show that, since the Bellaterra graphs have small diameter, so do the Aleshin graphs. In fact, it can also be used to show that if the Bellaterra graphs form a (two-sided) expander family, so do the Aleshin graphs. In other words, Conjecture 1.3 implies Conjecture 1.2.

11.3. A tree automorphism  $\alpha : A^* \rightarrow A^*$  is spherically transitive if and only if it is conjugate in  $\text{Aut}(A^*)$  to the adding machine  $\rho$ , i.e., the automorphism which interprets a word in  $A^n$  as the base- $|A|$  representation of a number modulo  $|A|^n$ , and adds one to that number. The adding machine is an automatic automorphism, e.g., the binary adding machine is pictured in Figure 4.

One might hope that whenever an automatic automorphism  $\alpha \in \text{FAut}(A^*)$  is conjugate to  $\rho$  in  $\text{Aut}(A^*)$ , it is also conjugate to  $\rho$  in  $\text{FAut}(A^*)$ . If so, we would have an algorithm for determining whether a given automatic automorphism is transitive. In fact, since we can enumerate the transitive cyclic automata, it would be enough if every transitive  $\alpha \in \text{FAut}(A^*)$  were conjugate in  $\text{FAut}(A^*)$  to some cyclic automorphism.

However, Example 10.5 suggests that, in the dual of the automaton in Figure 9,  $\sigma_0$  is transitive but not conjugate in  $\text{FAut}(A^*)$  to any cyclic automaton, in particular to  $\rho$ . However, we prove that  $\sigma_0$  is not conjugate to a cyclic automaton, nor prove that it is actually transitive.

**Problem 11.1.** *Exhibit a transitive  $\alpha \in \text{FAut}(A^*)$  which is not conjugate (in  $\text{FAut}(A^*)$ ) to a cyclic  $\beta \in \text{FAut}(A^*)$ . (Or prove that there is no such  $\alpha$ .)*

**Problem 11.2.** *Characterize the automorphisms in  $\text{FAut}(A^*)$  which are conjugate in  $\text{FAut}(A^*)$  to a cyclic automorphism.*

We can, however, exhibit a cyclic  $\alpha \in \text{FAut}(A^*)$  which is not conjugate in  $\text{FAut}(A^*)$  to the adding machine  $\rho$ :

**Proposition 11.3.** *Let  $\mathcal{M} = (Q, A, \tau, \sigma)$  be the dual of the automaton in Figure 6b, where  $Q = \{0, 1\}$  and  $A = \{a, b, c\}$ . Then  $\sigma_1$  acts transitively on  $A^*$ , but there is no  $\kappa \in \text{FAut}(A^*)$  such that  $\kappa^{-1}\sigma_1\kappa = \rho$*

*Sketch of proof:* Given an eventually periodic word  $w \in A^*$ , we let  $h(w)$  denote the smallest number  $n$  such that  $w$  is periodic after the first  $n$  letters.

Note that if  $\rho$  is the adding machine, then for any eventually periodic word  $v \in A^\infty$ , we have

$$h(\rho^n(v)) = O(\log n).$$

Moreover, after a finite number of steps, the periodic part of  $\rho^n(v)$  stabilizes. It follows that for any  $\kappa \in \text{FAut}(A^*)$ , we have

$$h(\kappa\rho^n(v)) = O(\log n)$$

and since this applies to any  $v$ ,

$$h(\kappa\rho^n\kappa^{-1}(v)) = O(\log n)$$

On the other hand, taking  $\alpha = \sigma_1$ , we can check that if we read  $w \in A^*$  as a balanced ternary number (with  $a = -1, c = 0, b = 1$ ), we have

$$\alpha(w) = \frac{w-1}{2}.$$

It follows that for  $w = ccc\dots$ ,

$$h(\alpha^{-n}(w)) \sim (\log_3 2)n$$

Thus  $\alpha^{-1}$  and  $\rho$  are not conjugate in  $\text{FAut}(A^*)$ . It is easy to check that  $\rho$  and  $\rho^{-1}$  are conjugate, so  $\alpha$  and  $\rho$  are not conjugate in  $\text{FAut}(A^*)$ .  $\square$

11.4. More generally, an open problem is the classification of conjugacy classes in  $\text{FAut}(A^*)$ . The conjugacy classes of  $\text{Aut}(A^*)$  can be described in terms of orbit trees [GNS]. This tree captures the information about the orbits of an automorphism  $\alpha \in \text{Aut}(A^*)$ , e.g. a ray with few branches in the orbit tree corresponds to a sequence of quickly growing orbits. Information about this tree can tell us whether we can apply, e.g., Theorem 8.3.

Of course, not all orbit trees arise from elements of  $\text{FAut}(A^*)$ , since there are uncountably many. Moreover, not all automatic automorphisms with the same orbit tree are conjugate in  $\text{FAut}(A^*)$ , as seen in Proposition 11.3.

In [BBSZ], the problem is solved for *bounded automorphisms*, and more generally automorphisms with *finite orbit-signalizer*. Such “small” automorphisms are unlikely to give expanders, so we are interested in the other end of the spectrum, automorphisms with many nontrivial sections on every level.

11.5. *Automaton groups*, i.e., groups of the form  $G_{\mathcal{M}}$  for some Mealy automaton  $\mathcal{M}$ , are of independent interest in group theory.<sup>6</sup> A famous example is the *Grigorchuk group*, which is the first known group whose growth function is intermediate between polynomial and exponential (see [GP, G1]). For more on automaton groups, see [BGŠ, GNS, Nek].

11.6. The structure of  $G_{\mathcal{M}}$  as an abstract group can give us information on whether or not the graphs  $\Gamma_{\mathcal{M},n}$  form a family of expanders. For example, if  $G_{\mathcal{M}}$  is amenable then  $\{\Gamma_{\mathcal{M},n}\}_{n=1}^\infty$  is not a family of expanders [Lub, 3.3.7]. We already used this fact in Example 10.3 to show that the Schreier graphs of the automaton defined there are not expanders.

---

<sup>6</sup>Note that the term *automatic group* has a different meaning in the literature, one we do not use in this paper.

11.7. On the other hand, sometimes the structure of  $G_{\mathcal{M}}$  is enough to guarantee that  $\{\Gamma_{\mathcal{M},n}\}_{n=1}^{\infty}$  is a family of expanders. Notably, if  $\Gamma_1, \Gamma_2, \dots$  are Schreier graphs (with respect to a fixed generating set) of a group with *Kazhdan property* (T), and  $|\Gamma_i| \rightarrow \infty$ , then these graphs must form a family of expanders [Lub, 3.3.4]. This fact was used by Margulis to give the first explicit construction of expanders [Mar].

In [GM], it was shown that there are Mealy automata  $\mathcal{M}$  for which  $G_{\mathcal{M}}$  has property (T), so Mealy automata can be used to construct expander families. The groups  $G_{\mathcal{A}}$  and  $G_{\mathcal{B}}$  do not have property (T), so this approach is not sufficient to prove Conjectures 1.2 and 1.3.

11.8. In a recent preprint, [MSS], the ideas of [BL] were extended to construct families of bipartite Ramanujan graphs (i.e., expander graphs with optimal spectral gap) of arbitrary degree. The construction uses a new technique to pick a particular 2-lift of a graph which does not introduce any new large eigenvalues. We should note that this construction is not *very explicit*, in the sense given above.

11.9. In [G2, Section 10], Grigorchuk shows that in a certain formal sense, the Aleshin and Bellaterra automata are examples of *asymptotic expanders*, thus giving further evidence to Conjectures 1.2 and 1.3. He also states these conjectures as open problems, and suggests that a sequence of Schreier graphs constructed by a finite automaton cannot be Ramanujan.

**Acknowledgements** We are grateful to Slava Grigorchuk, Volodia Nekrashevych, Yehuda Shalom and Terry Tao for helpful discussions. The second author was partially supported by the NSF.

## REFERENCES

- [A] V. Aleshin, A free group of finite automata (in Russian), *Vestnik Moskov. Univ. Ser. I Mat. Mekh.* **4** (1983), 12–14.
- [BGŠ] L. Bartholdi, R. Grigorchuk and Z. Šunić, Branch groups, in *Handbook of algebra*, Vol. 3, North-Holland, Amsterdam, 2003, 989–1112.
- [BŠ] L. Bartholdi and Z. Šunić, Some solvable automaton groups, *Contemp. Math.* **394**, AMS, Providence, RI, 2006.
- [BL] Y. Bilu and N. Linial, Lifts, discrepancy and nearly optimal spectral gap, *Combinatorica* **26** (2006), 495–519.
- [BBSZ] I. Bondarenko, N. Bondarenko, S. Sidki and F. Zapata, On the conjugacy problem for finite-state automorphisms of regular rooted trees, *Groups Geom. Dyn.* **7** (2013), 323–355.
- [B+] I. Bondarenko, R. Grigorchuk, R. Kravchenko, Y. Muntyan, V. Nekrashevych, D. Savchuk and Z. Šunić, On classification of groups generated by 3-state automata over a 2-letter alphabet, *Algebra Discrete Math.* 2008, 1–163.
- [GNS] P. Gawron, V. Nekrashevych and V. Sushchansky, Conjugation in tree automorphism groups, *Internat. J. Algebra Comput.* **11** (2001), 529–547.
- [GM] Y. Glasner and S. Mozes, Automata and square complexes, *Geom. Dedicata* **111** (2005), 43–64.
- [G1] R. I. Grigorchuk, Solved and unsolved problems around one group, in *Infinite Groups: Geometric, Combinatorial and Dynamical Aspects*, Birkhäuser, Basel, 2005, 117–218.
- [G2] R. I. Grigorchuk, Some problems of the dynamics of group actions on rooted trees, *Proc. Steklov Inst. Math.* **273** (2011), 64–175.
- [GNS] R. Grigorchuk, V. Nekrashevich and V. Sushchanskii, Automata, dynamical systems, and groups, *Proc. Steklov Inst. Math.* **231** (2000), 128–203.
- [GP] R. I. Grigorchuk and I. Pak, Groups of intermediate growth, an introduction, *Enseign. Math.* **54** (2008), 251–272.
- [HLW] S. Hoory, N. Linial and A. Wigderson, Expander graphs and their applications, *Bull. AMS* **43** (2006), 439–561.
- [Lub] A. Lubotzky, *Discrete Groups, Expanding Graphs, and Invariant Measures*, Birkhäuser, Basel, 1994.
- [Mar] G. Margulis, Explicit constructions of expanders, *Problemy Peredači Informacii* **9** (1973), 71–80.
- [MSS] A. Marcus, D. Spielman and N. Srivastava, Interlacing Families I: Bipartite Ramanujan Graphs of All Degrees, [arXiv:1304.4132](https://arxiv.org/abs/1304.4132).
- [Nek] V. Nekrashevych, *Self-similar Groups*, AMS, Providence, RI, 2005.
- [St] B. Steinberg, Testing spherical transitivity in iterated wreath products of cyclic groups, [arXiv:0607563](https://arxiv.org/abs/0607563).

- [Tao] T. Tao, *Basic theory of expander graphs*, 2 December 2011 blog entry; available electronically at <http://tinyurl.com/d6hhlge>
- [Vad] S. Vadhan, *Pseudorandomness*, monograph draft; available electronically at <http://tinyurl.com/o9e7qa8>
- [VV] M. Vorobets and Y. Vorobets, On a free group of transformations defined by an automaton, *Geom. Dedicata* **124** (2007), 237–249.

## SPHERICAL TRANSITIVITY OF MEALY AUTOMATA

ANTON MALYSHEV\*

## 1. DEFINITIONS

**Definition 1.1.** A *Mealy automaton*  $\mathcal{A} = (X, A, \phi, \psi)$  is a pair of sets  $X$ ,  $A$ , and functions  $\phi : X \times A \rightarrow A$ ,  $\psi : X \times A \rightarrow X$ . Elements of  $X$  are called *states* of  $\mathcal{A}$ , and  $A$  is called the *alphabet* of  $\mathcal{A}$ . [[Define dual, invertible, reversible, bireversible, binary automaton]].

Fixing a Mealy automaton  $\mathcal{A} = (X, A, \phi, \psi)$ , every state  $x \in X$  defines a map  $\Phi_x : A^* \rightarrow A^*$ , defined recursively by

$$\Phi_x(aw) = \phi_x(a)\Phi_{\psi_a(x)}(w)$$

**Theorem 1.2.**

---

\*Department of Mathematics, UCLA, Los Angeles, CA, 90095. Email: [amalyshv@math.ucla.edu](mailto:amalyshv@math.ucla.edu).